

V1T Privacy Policy

The v1t.tech platform and the V1T mobile apps for Android and iOS · version of 25.09.2026

1. General provisions

- 1.1. This Policy sets out how information about users of the «V1T» video monitoring system for vehicles and heavy equipment is processed and protected: the <https://v1t.tech> web platform (the Platform) and the «V1T» mobile apps for Android and iOS (the App). The Platform and the App are together referred to as the System. The System is provided by V1-TECHNOLOGY LLC (the Company).
- 1.2. The System is intended for employees of organisations that have entered into a licence agreement with the Company (<https://v1tech.ru/oferta/>). There is no self-registration in the System: accounts are created by the client organisation (the Licensee) or by the Company on its instruction. The System contains no function for creating an account independently.
- 1.3. The Company processes personal data in accordance with Federal Law No. 152-FZ of 27 July 2006 «On Personal Data» of the Russian Federation.
- 1.4. Roles of the parties in the processing of personal data: for data of the client organisation's employees and data collected by its on-board equipment, the client organisation is the data controller; the Company processes such data on its instruction under the licence agreement (clause 4.6 of the public offer) in accordance with part 3 of article 6 of 152-FZ.
- 1.5. Legal grounds for processing: performance of the licence agreement (clause 5 part 1 article 6 of 152-FZ); instruction of the controller (part 3 article 6 of 152-FZ); consent of the data subject – for enquiries sent to the Company on the user's own initiative (clause 1 part 1 article 6 of 152-FZ).
- 1.6. Processing is carried out by automated means and includes collection, recording, systematisation, accumulation, storage, adjustment (updating, modification), retrieval, use, transfer (provision, access), blocking, erasure and destruction of personal data.
- 1.7. This Policy applies to the System. The processing of personal data of visitors to the <https://v1tech.ru> website is governed by a separate document: <https://v1tech.ru/en/privacy-site/>

- 1.8. By using the System, the user confirms that they have read this Policy.

2. What data the system processes

- 2.1. Credentials and profile. The login and password are entered by the user when signing in to the Platform or the App and are sent to the Company's server over a secure connection (HTTPS) for verification. After sign-in the System receives and stores an access token and profile details: user name, role, organisation and, where an integration is enabled, the telematics login specified by the user. In the App the token is kept in the app's private storage on the device; in the Platform it is kept in the browser session. The password is not stored in clear text.
- 2.2. Monitoring system data. The System displays data that the client organisation collects with its on-board terminals: location and routes of vehicles, live and archived video, photographs and video recordings of alert events, sensor readings, and information about terminals and vehicles. This data belongs to the client organisation, is stored on the Company's servers and is delivered to the user only after authorisation and within the limits of their access rights.
- 2.3. Exported files. At the user's command the System saves video recordings, photographs and reports to the user's device. Such files remain in the device storage under the user's control.
- 2.4. Technical data. When the System contacts the Company's servers, the device IP address, the App version or the browser type and version, the operating system type and the session identifier are transmitted automatically. This information is used to maintain the connection, to protect against unauthorised access and to diagnose faults.
- 2.5. Settings, cache and cookies. The device stores the System settings (the selected connection environment, map style, local map diagnostics log) and a cache of server responses to speed up start-up. The Platform additionally uses cookies that are strictly necessary for the personal account to work: the session identifier and interface preferences. No cookies are used for analytics, profiling or advertising.
- 2.6. User activity log. The Platform keeps a log of actions in the personal account: sign-in and sign-out, viewing and exporting recordings, changes to settings and access rights, with the date, time and IP address. The log is used to investigate security incidents, to establish accountability and to meet the requirements of article 19 of 152-FZ. It is accessible to the client organisation's administrators and to authorised Company staff.

- 2.7.** Notifications. If the user chooses to enable them, the System sends event notifications and reports to an e-mail address, to the MAX messenger or to other messengers specified by the user. The delivery channel and its content are chosen by the user; no notifications are sent unless the user configures them.
- 2.8.** The System does not request access to the user device location, camera, microphone, contacts or photo gallery; it does not collect health data, advertising identifiers, browsing or search history; and it does not use third-party analytics, advertising networks or trackers.
- 2.9.** Biometric personal data is not processed in any form. The System does not perform facial recognition and does not identify a person by image, voice or any other physiological or biological characteristic. Photographs and video recordings received from the on-board equipment are a record of events and are not used to identify people.
- 2.10.** Maps. The map layer is used to display on the map the location of the client organisation's vehicles and on-board video recorders. The System does not determine, request or transmit the location of the user's own device (smartphone, tablet or computer).

3. Purposes of processing

- giving the user access to the monitoring system of their organisation;
- displaying vehicles on the map and playing back video and alert events;
- delivering event notifications through the channels chosen by the user;
- keeping accounts secure, separating access rights and protecting against unauthorised access;
- supporting users and resolving faults;
- checking for App updates.

4. Transfer of data to third parties

- 4.1.** The Company does not sell users' personal data and does not transfer it to third parties for their own purposes.
- 4.2.** The map layer is loaded from the Company's servers (<https://v1t.tech/tiles>). No third-party map services are used: the device IP address, coordinates and any other user data are not transmitted to them.

- 4.3. Update information is retrieved by the App from the Company's server (<https://object.v1tech.ru>); only the technical data listed in clause 2.4 is transmitted.
- 4.4. Notifications are delivered through the channel the user has chosen. Where e-mail or a messenger is selected, the content of the notification is passed to the operator of that service and processed by it under its own rules and policy. The Company does not control such processing. The user may switch off notifications or change the delivery channel at any time in the System settings.
- 4.5. The Company does not carry out cross-border transfer of personal data. If the user has selected a notification channel operated outside the Russian Federation, the transfer is made at the user's own initiative and to the extent determined by their own settings.
- 4.6. Data may be disclosed to authorised state bodies on the grounds and in the manner established by the legislation of the Russian Federation.

5. Storage and protection

- 5.1. The servers holding the monitoring system data and users' personal data are located in the territory of the Russian Federation (part 5 article 18 of 152-FZ).
- 5.2. Data transfer between the System and the Company's servers is protected by TLS (HTTPS/WSS).
- 5.3. The access token and profile are kept in the App's private storage, inaccessible to other apps, or in the browser session, and are deleted when the user signs out, uninstalls the App or ends the session.
- 5.4. Retention periods for monitoring system data (video, photographs, routes) are determined by the licence agreement with the client organisation and by its tariff settings.
- 5.5. User credentials are kept for as long as the account exists in the system and are destroyed within 90 days after the account is blocked or deleted. The user activity log is kept for no longer than 12 months.
- 5.6. No decisions producing legal effects for the user are taken solely on the basis of automated processing of personal data (article 16 of 152-FZ).

| 6. User rights

- 6.1.** The user is entitled to obtain information about the processing of their data, to require its adjustment, blocking or erasure, and to withdraw consent to processing, by contacting their client organisation (as the controller) or the Company at info@v1tech.ru
- 6.2.** An account and the data associated with it are deleted on request. The procedure, the data covered and the time limits are set out on a separate page: <https://v1tech.ru/en/account-delete/>
- 6.3.** The person responsible for organising the processing of personal data at the Company is the head of the technical support service. Enquiries are sent to info@v1tech.ru or by post to the address given in section 8.
- 6.4.** A reply to an enquiry is sent within 30 days of its receipt at the latest.

| 7. Changes to this policy

The Company may amend this Policy. A new version takes effect once published on this page. The current version is always available at <https://v1tech.ru/en/privacy/> (Russian version: <https://v1tech.ru/privacy/>). In the event of any discrepancy between the Russian and English versions, the Russian version prevails.

8. Contacts

V1-TECHNOLOGY Limited Liability Company

OGRN	1187746043726
INN (TIN)	7725416190
Registered address	2 Universitetskaya St., Obninsk, Kaluga Region 249035, Russia
Postal address	71/5 bldg. 2 Pyatnitskaya St., office 409, Moscow 115054, Russia
Phone	+7 (800) 222-35-77
E-mail	info@v1tech.ru
Personal data enquiries	info@v1tech.ru